

ESSENTIAL ARITY GAP OF BOOLEAN FUNCTIONS

SLAVCHO SHTRAKOV

ABSTRACT. In this paper we investigate the Boolean functions with maximum essential arity gap. Additionally we propose a simpler prove of an important theorem proved by M. Couceiro and E. Lehtonen in [3]. They used the Zhegalkin's polynomials as normal forms for Boolean functions and describe the functions with essential arity gap equals 2. We use Full Conjunctive Normal Forms instead of these polynomials which allow us to simplify the proofs and to obtain several combinatorial results, concerning the Boolean functions with a given arity gap. The Full Conjunctive Normal Forms are sum of conjunctions also, in which all variables occur.

1. INTRODUCTION

Essential variables of functions are studied by several authors [1, 2, 4]. In this paper we consider the problem for simplification of functions by identification of variables. This problem is discussed in the work of O. Lupanov, Yu. Breitbart, A. Salomaa, M. Couceiro, E. Lehtonen, etc. for Boolean functions and by K. Chimev for arbitrary discrete functions. Similar problems for terms and universal algebra are studied by the author and K. Denecke [7]. Essential input variables for tree automata are discussed in [6]. The problems concerning essential arity gap of functions are discussed in [3]. Here we study and count the Boolean functions, which have maximum arity gap. Note that if a function f has greater essential arity gap than the essential arity gap of another function g , then f has a simpler automata realization than g . This fact is of a great importance in theoretical and applied computer science and modeling.

2. ESSENTIAL VARIABLES IN BOOLEAN FUNCTIONS

Let $B = \{0, 1\}$ be the set (ring) of the residuums modulo 2. An n -ary Boolean function (operation) is a mapping $f : B^n \rightarrow B$ for some natural number n , called *arity* of f . The set of all such functions is denoted by P_2^n .

A variable x_i is called *essential* in f , or f *essentially depends* on x_i , if there exist values $a_1, \dots, a_n, b \in B$, such that

$$f(a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n) \neq f(a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_n).$$

The set of essential variables in a function f is denoted by $Ess(f)$ and the number of essential variables in f is denoted by $ess(f) = |Ess(f)|$. The variables from $X = \{x_1, \dots, x_n\}$ which are not essential in $f \in P_2^n$ are called *fictive* and the set of fictive variables in f is denoted by $Fic(f)$.

2000 *Mathematics Subject Classification.* Primary: 94C10; Secondary: 06E30
ACM-Computing Classification System (1998) : G.2.0.

Key words and phrases. essential variable, identification minor, essential arity gap.

Let x_i and x_j be essential variables in f . We say that the function g is obtained from $f \in P_2^n$ by *identification of a variable x_i with x_j* , if

$$g(x_1, \dots, x_n) = f(x_1, \dots, x_{i-1}, x_j, x_{i+1}, \dots, x_n) = f(x_i = x_j).$$

Briefly, when g is obtained from f , by identification of the variable x_i with x_j , we will write $g = f_{i \leftarrow j}$ and g is called *the identification minor of f* . The set of all identification minors of f will be denoted by $Min(f)$.

For completeness of our consideration we allow to obtain identification minors when x_i or x_j are not essential in f , also. Thus if x_i does not occur in f , then we define $f_{i \leftarrow j} := f$.

Clearly, $ess(f_{i \leftarrow j}) \leq ess(f)$, because $x_i \notin Ess(f_{i \leftarrow j})$, even though it may be essential in f .

For a function $f \in P_2^n$ the *essential arity gap* (shortly *arity gap*) of f is defined as follows

$$gap(f) := ess(f) - \max_{g \in Min(f)} ess(g).$$

It is not difficult to see that the functions with "huge" gap, are more simple for realization by switching circuits and functional schemas in theoretical and applied computer science.

Let us denote by G_p^m the set of all functions in P_2^n which essentially depend on m variables and have gap equals to p i.e. $G_p^m = \{f \in P_2^n \mid ess(f) = m \text{ \& } gap(f) = p\}$, with $m \leq n$.

An upper bound of $gap(f)$ for Boolean functions is found by K.Chimev, A. Salomaa and O. Lupanov [2, 4, 5]. It is shown that $gap(f) \leq 2$, when $f \in P_2^n$, $n \geq 2$.

This result is generalized for arbitrary finite valued functions in [3]. It is proved that $gap(f) \leq k$ for all $f \in P_k^n$, $n \geq k$.

Let $m \in N$, $0 \leq m \leq 2^n - 1$ be an integer. It is well known that for every $n \in N$, there is an unique finite sequence $(\alpha_1, \dots, \alpha_n) \in B^n$ such that

$$(1) \quad m = \alpha_1 2^{n-1} + \alpha_2 2^{n-2} + \dots + \alpha_n.$$

The equation (1) is known as the presentation of m in binary positional numerical system. One briefly writes $m = \overline{\alpha_1 \alpha_2 \dots \alpha_n}$ instead (1).

For a variable x and $\alpha \in B$, we define the following important function

$$x^\alpha = \begin{cases} 1 & \text{if } x = \alpha \\ 0 & \text{if } x \neq \alpha. \end{cases}$$

This function is used in many investigations, concerning the applications of discrete functions in computer science [2].

There are many normal forms for representation of functions from P_2^n . In this paper we will use the *Full Conjunctive Normal Form (FCNF)* for studying the essential arity gap of functions. This normal form is based on the table representation of Boolean functions.

The next two theorems are in the basis of the Theory of Boolean functions, and they are well known.

Theorem 2.1. *Each function $f \in P_2^n$ can be uniquely represented in FCNF as follows*

$$(2) \quad f(x_1, \dots, x_n) = a_0 \cdot x_1^0 \dots x_n^0 \oplus \dots a_m \cdot x_1^{\alpha_1} \dots x_n^{\alpha_n} \oplus \dots a_{2^n-1} \cdot x_1^1 \dots x_n^1$$

where $m = \overline{\alpha_1 \dots \alpha_n}$, $a_m \in B$ and " \oplus ", and " \cdot " are the operations addition and multiplication modulo 2 in the ring B .

Theorem 2.2. *A variable x_i is fictive in the function $f \in P_2^n$, if and only if*

$$\begin{aligned} f(x_1, \dots, x_n) &= \\ &= x_i^0 \cdot f_1(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \oplus x_i^1 \cdot f_2(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n), \end{aligned}$$

with $f_1 = f_2$ and $x_i \notin \text{Ess}(f_j)$, where $f_j \in P_2^{n-1}$, for $j = 1, 2$.

The next lemmas characterize the relation between the identification minors of Boolean functions.

Lemma 2.1. *Let $f, g \in P_2^n$ be two Boolean functions represented by their FCNF as follows*

$$f = \bigoplus_{m=0}^{2^{n-1}-1} a_m \cdot x_1^{\alpha_1} \dots x_n^{\alpha_n} \quad \text{and} \quad g = \bigoplus_{m=0}^{2^{n-1}-1} b_m \cdot x_1^{\alpha_1} \dots x_n^{\alpha_n},$$

where $m = \overline{\alpha_1 \dots \alpha_n}$. If $f_{i \leftarrow j} = g_{i \leftarrow j}$ and $\alpha_i = \alpha_j$ for some i, j with $1 \leq j < i \leq n$, then $a_m = b_m$.

Proof. Without loss of generality we will prove the lemma, for $i = 2$ and $j = 1$. Since $f_{2 \leftarrow 1} = g_{2 \leftarrow 1}$ we have

$$f(x_1, x_1, x_3, \dots, x_n) = g(x_1, x_1, x_3, \dots, x_n).$$

Hence

$$a_m = f(\alpha_1, \alpha_1, \alpha_3, \dots, \alpha_n) = g(\alpha_1, \alpha_1, \alpha_3, \dots, \alpha_n) = b_m. \quad \blacksquare$$

Lemma 2.2. *Let $f, g \in P_2^n$ be two functions, depending essentially on n , $n \geq 3$ variables. If $f_{i \leftarrow j} = g_{i \leftarrow j}$ for all i, j , $1 \leq j < i \leq n$, then $f = g$.*

Proof. Let f and g be functions represented by their FCNF as in Lemma 2.1. Let $m = \alpha_1 \cdot 2^{n-1} + \alpha_2 \cdot 2^{n-2} + \dots + \alpha_n$ be an arbitrary integer from $\{0, 1, \dots, 2^n - 1\}$. Since $n \geq 3$ there exist two natural numbers i, j with $1 \leq j < i \leq n$ and $\alpha_i = \alpha_j$. From Lemma 2.1 we obtain

$$a_m = f(\alpha_1, \alpha_2, \dots, \alpha_n) = g(\alpha_1, \alpha_2, \dots, \alpha_n) = b_m. \quad \blacksquare$$

Consequently, we have $f = g$.

Example 2.1. *Let us consider the Boolean functions $f = x_1^0 x_2^0 \oplus x_1^1 x_2^1$ and $g = x_1^0 x_2^0 \oplus x_1^1 x_2^1$. It is easy to see that for all i, j , $1 \leq j < i \leq n$ we have $f_{i \leftarrow j} = g_{i \leftarrow j} = x_1^0$, but $f \neq g$. This example shows that $n \geq 3$ is an essential condition in Lemma 2.2.*

3. ESSENTIAL ARITY GAP OF BOOLEAN FUNCTIONS

For Boolean functions $\neg(x)$ denotes the unary operation negation, i.e.

$$\neg x = x^0 = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x \neq 0. \end{cases}$$

Proposition 3.1. *For each Boolean function f the following sentences are held:*

- (i) $\text{gap}(f(x_1, \dots, x_n)) = \text{gap}(f(\neg x_1, \dots, \neg x_n))$;
- (ii) $\text{gap}(f(x_1, \dots, x_n)) = \text{gap}(\neg(f(x_1, \dots, x_n)))$;
- (iii) $\text{gap}(f(x_1, \dots, x_n)) = \text{gap}(f(x_{\pi(1)}, \dots, x_{\pi(n)}))$, where $\pi : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ is a permutation of the set $\{1, \dots, n\}$;
- (iv) $\text{ess}(f_{i \leftarrow j}) = \text{ess}(f_{j \leftarrow i})$ for all i, j , $1 \leq j < i \leq n$.

Note that the last two assertions (iii) and (iv) are valid in more general case of k -valued functions.

For any natural number $n, n \geq 2$ we define the following two sets:

$$Od_2^n := \{\alpha_1 \alpha_2 \dots \alpha_n \in \{0, 1\}^n \mid \alpha_1 \oplus \alpha_2 \oplus \dots \oplus \alpha_n = 1\}$$

and

$$Ev_2^n := \{\alpha_1 \alpha_2 \dots \alpha_n \in \{0, 1\}^n \mid \alpha_1 \oplus \alpha_2 \oplus \dots \oplus \alpha_n = 0\}.$$

Clearly, $\alpha_1 \alpha_2 \dots \alpha_n \in Od_2^n$ if and only if the number of 1's in $\alpha_1 \alpha_2 \dots \alpha_n$ is odd, and $\alpha_1 \alpha_2 \dots \alpha_n \in Ev_2^n$ when this number is even.

Proposition 3.2. *For any $n, n \geq 4$, if*

$$f = \bigoplus_{\alpha_1 \dots \alpha_n \in Od_2^n} x_1^{\alpha_1} \dots x_n^{\alpha_n} \quad \text{or} \quad f = \bigoplus_{\alpha_1 \dots \alpha_n \in Ev_2^n} x_1^{\alpha_1} \dots x_n^{\alpha_n},$$

then $f \in G_2^n$.

Proof. Without loss of generality let us assume that $f = \bigoplus_{\alpha_1 \dots \alpha_n \in Od_2^n} x_1^{\alpha_1} \dots x_n^{\alpha_n}$. We have to show that $ess(f_{i \leftarrow j}) \leq n - 2$ for all $i, j, 1 \leq j < i \leq n$. Without loss of generality, again we will assume $i = 2$ and $j = 1$. Then we have

$$\begin{aligned} f_{2 \leftarrow 1} &= \bigoplus_{\alpha_1, \alpha_3, \dots, \alpha_n \in Od_2^{n-1}} x_1^{\alpha_1} x_3^{\alpha_3} \dots x_n^{\alpha_n} = \\ &= x_1^0 \cdot \left[\bigoplus_{\alpha_3, \dots, \alpha_n \in Od_2^{n-2}} x_3^{\alpha_3} \dots x_n^{\alpha_n} \right] \oplus x_1^1 \cdot \left[\bigoplus_{\alpha_3, \dots, \alpha_n \in Od_2^{n-2}} x_3^{\alpha_3} \dots x_n^{\alpha_n} \right] = \\ &= \bigoplus_{\alpha_3, \dots, \alpha_n \in Od_2^{n-2}} x_3^{\alpha_3} \dots x_n^{\alpha_n}. \end{aligned}$$

The result is the same, when $\alpha_1 \dots \alpha_n \in Ev_2^n$. ■

We are going to describe the set G_2^n for $n = 2, 3, 4$. The results for $n = 4$ can be easily extended in the more general case $n \geq 4$.

Theorem 3.1. *Let $f \in P_2^2$. Then $f \in G_2^2$ if and only if*

$$f = a_0.(x_1^0 x_2^0 \oplus x_1^1 x_2^1) \oplus a_1.x_1^0 x_2^1 \oplus a_2.x_1^1 x_2^0, \quad \text{with } a_1 \neq a_0 \quad \text{or} \quad a_2 \neq a_0.$$

Proof. Let $f = a_0.x_1^0 x_2^0 \oplus a_1.x_1^0 x_2^1 \oplus a_2.x_1^1 x_2^0 \oplus a_3.x_1^1 x_2^1$. The variables x_1 and x_2 are essential in f if and only if $(a_0, a_1) \neq (a_2, a_3)$ and $(a_0, a_2) \neq (a_1, a_3)$. Consider the identification minor $h := f_{2 \leftarrow 1} = a_0.x_1^0 \oplus a_3.x_1^1$ of f . We need $ess(h) = 0$ and from Theorem 2.2 it follows $a_0 = a_3$. If we suppose that $a_1 = a_2 = a_0$, then $f(x_1, x_2) = a_0$ which contradicts $ess(f) = 2$. ■

Corollary 3.1. *There are 6 functions in G_2^2 , i.e. $|G_2^2| = 6$.*

Proof. Let $a_0 \in \{0, 1\}$. For a_1 and a_2 there are 3 possible choices, which satisfy Theorem 3.1. The both cases $a_1 = a_2 = a_0 = 0$ and $a_1 = a_2 = a_0 = 1$ are impossible because then $ess(f) < 2$, since Theorem 2.2. ■

Corollary 3.2. *If $f = a_0.x_1^0 x_2^0 \oplus a_1.x_1^0 x_2^1 \oplus a_2.x_1^1 x_2^0 \oplus a_3.x_1^1 x_2^1 \in P_2^2$ then $ess(f_{2 \leftarrow 1}) = 0$ if and only if $a_0 = a_3$.*

The next step is to describe the functions which essentially depend on 3 variables and have essential arity gap equal to 2.

Theorem 3.2. *Let f be a Boolean function of three variables. Then $f \in G_2^3$ if and only if it can be represented in one of the following special forms:*

$$(3) \quad f = x_3^\alpha(x_1^0x_2^1 \oplus x_1^1x_2^0) \oplus x_1^\beta x_2^\beta,$$

or

$$(4) \quad f = x_3^\alpha(x_1^0x_2^0 \oplus x_1^1x_2^1) \oplus x_3^{\neg(\alpha)}(x_1^0x_2^1 \oplus x_1^1x_2^0),$$

where $\alpha, \beta \in \{0, 1\}$.

Proof. Note that the presentation of f in (4) is symmetric with respect to the variables, but in (3) f is not symmetric with respect to the variables x_1 and x_3 . So, the theorem asserts that $f \in G_2^3$ if and only if f can be represented in one of the forms (3) or (4), after a suitable permutation of the variables.

" \Leftarrow " Clearly, x_1, x_2 and x_3 are essential variables in the functions of the right sides of (3) and (4). To see that $f \in G_2^3$ it is enough to do immediate checking. Thus for the function f in (3) we have $f_{2 \leftarrow 1} = x_1^\beta$,

$$f_{3 \leftarrow 1} = \begin{cases} x_1^\beta & \text{if } \beta = \alpha \\ x_2^\beta & \text{if } \beta \neq \alpha \end{cases} \quad \text{and} \quad f_{3 \leftarrow 2} = \begin{cases} x_2^\beta & \text{if } \beta = \alpha \\ x_1^\beta & \text{if } \beta \neq \alpha. \end{cases}$$

The functions f as in (4) are in G_2^3 because $x_i, x_j \notin \text{Ess}(f_{i \leftarrow j})$ for all i, j , $1 \leq j < i \leq 3$.

" \Rightarrow " Assume that $f \in G_2^3$. Let the FCNF of f is written as follows:

$$\begin{aligned} f &= x_3^0(a_0.x_1^0x_2^0 \oplus a_1.x_1^0x_2^1 \oplus a_2.x_1^1x_2^0 \oplus a_3.x_1^1x_2^1) \oplus \\ &\quad \oplus x_3^1(a_4.x_1^0x_2^0 \oplus a_5.x_1^0x_2^1 \oplus a_6.x_1^1x_2^0 \oplus a_7.x_1^1x_2^1) = \\ &= x_3^0.g(x_1, x_2) \oplus x_3^1.h(x_1, x_2). \end{aligned}$$

A. Suppose that $x_1 \in \text{Ess}(g_{2 \leftarrow 1})$ or $x_1 \in \text{Ess}(h_{2 \leftarrow 1})$. Then $x_1 \in \text{Ess}(f_{2 \leftarrow 1})$ because $f_{2 \leftarrow 1}(x_3 = 0) = g_{2 \leftarrow 1}$ and $f_{2 \leftarrow 1}(x_3 = 1) = h_{2 \leftarrow 1}$. Hence $f \in G_2^3$ implies $x_3 \notin \text{Ess}(f_{2 \leftarrow 1})$ i.e. $g_{2 \leftarrow 1} = h_{2 \leftarrow 1}$. Consequently, $a_0 = a_4$ and $a_3 = a_7$. Then we obtain

$$u = f_{3 \leftarrow 1} = a_0.x_1^0x_2^0 \oplus a_1.x_1^0x_2^1 \oplus a_6.x_1^1x_2^0 \oplus a_7.x_1^1x_2^1,$$

and

$$v = f_{3 \leftarrow 2} = a_0.x_1^0x_2^0 \oplus a_2.x_1^1x_2^0 \oplus a_5.x_1^0x_2^1 \oplus a_7.x_1^1x_2^1.$$

There are the following cases:

A.a. $x_1 \notin \text{Ess}(u)$. Hence $a_0 = a_6$ and $a_1 = a_7$.

A.a.1. If we suppose that $x_1 \notin \text{Ess}(v)$, then $a_0 = a_2$ and $a_5 = a_7$ implies (according Theorem 2.2) that $x_1, x_3 \notin \text{Ess}(f)$ and $f \notin G_2^3$.

A.a.2. If $x_2 \notin \text{Ess}(v)$, then $a_0 = a_5$ and $a_2 = a_7$. Note that if $a_0 = a_7$, then f has to be a constant. Hence $a_7 = \neg(a_0)$. Then we obtain

$$\begin{aligned} f &= a_0.[x_1^0x_2^0x_3^0 \oplus x_1^0x_2^0x_3^1 \oplus x_1^0x_2^1x_3^1 \oplus x_1^1x_2^0x_3^1] \oplus \\ &\quad \oplus \neg(a_0).[x_1^0x_2^1x_3^0 \oplus x_1^1x_2^0x_3^0 \oplus x_1^1x_2^1x_3^0 \oplus x_1^1x_2^1x_3^1] = \\ &= a_0[x_3^1(x_1^0x_2^1 \oplus x_1^1x_2^0) \oplus x_1^0x_2^0] \oplus \neg(a_0)[x_3^0(x_1^0x_2^1 \oplus x_1^1x_2^0) \oplus x_1^1x_2^1] \in G_2^3. \end{aligned}$$

Clearly, f is presented as in (3).

A.b. $x_2 \notin \text{Ess}(u)$. Hence $a_0 = a_1$ and $a_6 = a_7$.

A.b.1. If we suppose that $x_2 \notin \text{Ess}(v)$, then $a_0 = a_5$ and $a_2 = a_7$ implies (according Theorem 2.2) that $x_2, x_3 \notin \text{Ess}(f)$ and $f \notin G_2^3$.

A.b.2. If $x_1 \notin \text{Ess}(v)$, then $a_0 = a_2$ and $a_5 = a_7$. Again, if $a_0 = a_7$, then f has to be a constant. Hence $a_7 = \neg(a_0)$. Then we obtain

$$\begin{aligned} f &= a_0.[x_1^0 x_2^0 x_3^0 \oplus x_1^0 x_2^0 x_3^1 \oplus x_1^0 x_2^1 x_3^0 \oplus x_1^1 x_2^0 x_3^0] \oplus \\ &\quad \oplus \neg(a_0).[x_1^0 x_2^1 x_3^1 \oplus x_1^1 x_2^0 x_3^1 \oplus x_1^1 x_2^1 x_3^0 \oplus x_1^1 x_2^1 x_3^1] = \\ &= a_0[x_3^0(x_1^0 x_2^1 \oplus x_1^1 x_2^0) \oplus x_1^0 x_2^0] \oplus \neg(a_0)[x_3^1(x_1^0 x_2^1 \oplus x_1^1 x_2^0) \oplus x_1^1 x_2^1] \in G_2^3. \end{aligned}$$

Clearly, f is presented as in (3).

B. Let us suppose that $x_1 \notin \text{Ess}(g_{2 \leftarrow 1})$ and $x_1 \notin \text{Ess}(h_{2 \leftarrow 1})$. Then we have $g \in G_2^2$ and $h \in G_2^2$. From Theorem 3.1 it follows that

$$g(x_1, x_2) = a_0.(x_1^0 x_2^0 \oplus x_1^1 x_2^1) \oplus a_1.x_1^0 x_2^1 \oplus a_2.x_1^1 x_2^0,$$

and

$$h(x_1, x_2) = a_4.(x_1^0 x_2^0 \oplus x_1^1 x_2^1) \oplus a_5.x_1^0 x_2^1 \oplus a_6.x_1^1 x_2^0.$$

Then we obtain

$$u = f_{3 \leftarrow 1} = a_0.x_1^0 x_2^0 \oplus a_1.x_1^0 x_2^1 \oplus a_6.x_1^1 x_2^0 \oplus a_4.x_1^1 x_2^1,$$

and

$$v = f_{3 \leftarrow 2} = a_0.x_1^0 x_2^0 \oplus a_2.x_1^1 x_2^0 \oplus a_5.x_1^0 x_2^1 \oplus a_4.x_1^1 x_2^1.$$

B.a. $x_1 \notin \text{Ess}(u)$. Hence $a_0 = a_6$ and $a_1 = a_4$.

B.a.1. If $x_1 \notin \text{Ess}(v)$, then $a_0 = a_2$ and $a_4 = a_5$. Note that if $a_0 = a_4$, then f has to be a constant. Hence $a_4 = \neg(a_0)$. Then we obtain

$$\begin{aligned} f &= a_0.[x_1^0 x_2^0 x_3^0 \oplus x_1^1 x_2^0 x_3^0 \oplus x_1^1 x_2^0 x_3^1 \oplus x_1^1 x_2^1 x_3^0] \oplus \\ &\quad \oplus \neg(a_0).[x_1^0 x_2^0 x_3^1 \oplus x_1^0 x_2^1 x_3^0 \oplus x_1^0 x_2^1 x_3^1 \oplus x_1^1 x_2^1 x_3^1] = \\ &= a_0[x_1^1(x_2^0 x_3^1 \oplus x_2^1 x_3^0) \oplus x_2^0 x_3^0] \oplus \neg(a_0)[x_1^0(x_2^0 x_3^1 \oplus x_2^1 x_3^0) \oplus x_2^1 x_3^1] \in G_2^3. \end{aligned}$$

Clearly, f is presented as in (3).

B.a.2. If $x_2 \notin \text{Ess}(v)$, then $a_0 = a_5$ and $a_2 = a_4$. Again, if $a_0 = a_4$, then f has to be a constant. Hence $a_4 = \neg(a_0)$. Then we obtain

$$\begin{aligned} f &= a_0.[x_1^0 x_2^0 x_3^0 \oplus x_1^0 x_2^1 x_3^1 \oplus x_1^1 x_2^0 x_3^1 \oplus x_1^1 x_2^1 x_3^0] \oplus \\ &\quad \oplus \neg(a_0).[x_1^0 x_2^0 x_3^1 \oplus x_1^0 x_2^1 x_3^0 \oplus x_1^1 x_2^0 x_3^0 \oplus x_1^1 x_2^1 x_3^1] = \\ &= a_0[x_3^0(x_1^0 x_2^1 \oplus x_1^1 x_2^0) \oplus x_3^1(x_1^1 x_2^0 \oplus x_1^0 x_2^1)] \oplus \\ &\quad \oplus \neg(a_0)[x_3^1(x_1^0 x_2^0 \oplus x_1^1 x_2^1) \oplus x_3^0(x_1^1 x_2^0 \oplus x_1^0 x_2^1)] \in G_2^3. \end{aligned}$$

Clearly, f is presented as in (4).

B.b. $x_2 \notin \text{Ess}(u)$. Hence $a_0 = a_1$ and $a_6 = a_4$.

B.b.1. If we suppose that $x_1 \notin \text{Ess}(v)$, then $a_0 = a_2$ and $a_4 = a_5$ implies (according Theorem 2.2) that $x_1, x_2 \notin \text{Ess}(f)$ and $f \notin G_2^3$.

B.b.2. If $x_2 \notin \text{Ess}(v)$, then $a_0 = a_5$ and $a_2 = a_4$. Again, if $a_0 = a_4$, then f has to be a constant. Hence $a_4 = \neg(a_0)$. Then we obtain

$$\begin{aligned} f &= a_0.[x_1^0 x_2^0 x_3^0 \oplus x_1^0 x_2^1 x_3^0 \oplus x_1^0 x_2^1 x_3^1 \oplus x_1^1 x_2^1 x_3^0] \oplus \\ &\quad \oplus \neg(a_0).[x_1^0 x_2^0 x_3^1 \oplus x_1^1 x_2^0 x_3^0 \oplus x_1^1 x_2^0 x_3^1 \oplus x_1^1 x_2^1 x_3^1] = \\ &= a_0[x_2^1(x_1^0 x_3^1 \oplus x_1^1 x_3^0) \oplus x_1^0 x_3^0] \oplus \neg(a_0)[x_2^0(x_1^0 x_3^1 \oplus x_1^1 x_3^0) \oplus x_1^1 x_3^1] \in G_2^3. \end{aligned}$$

Clearly, f is presented as in (3). ■

Corollary 3.3. *Let $f \in P_2^3$. Then $\text{ess}(f_{i \leftarrow j}) \leq 1$ for all i, j , $1 \leq j < i \leq 3$ if and only if*

$$f = x_3^\alpha (x_1^0 x_2^0 \oplus x_1^1 x_2^1) \oplus a_1 \cdot x_1^0 x_2^1 x_3^0 \oplus a_2 \cdot x_1^1 x_2^0 x_3^0 \oplus \neg(a_2) \cdot x_1^0 x_2^1 x_3^1 \oplus \neg(a_1) \cdot x_1^1 x_2^0 x_3^1,$$

where $\alpha, a_1, a_2 \in \{0, 1\}$.

Proof. This Corollary summarizes all cases considered in Theorem 3.2. For instance if $\alpha = 1$, $a_1 = 0$ and $a_2 = 0$ we obtain

$$f = x_3^1 (x_1^0 x_2^0 \oplus x_1^1 x_2^1) \oplus x_1^0 x_2^1 x_3^1 \oplus x_1^1 x_2^0 x_3^1 = x_3^1.$$

This is the case **B.b.1**. ■

Corollary 3.4. $|G_2^3| = 10$.

Proof. As we have noted the functions f in the form (4) are symmetric with respect to their variables. Hence there are exactly two such functions, obtained for $\alpha = 1$ and $\alpha = 0$. These functions are realized in the case **B.a.2**.

Let us consider the functions f in the form (3) with $\alpha = \beta$. Then we have

$$f = x_1^0 x_2^1 x_3^\alpha \oplus x_1^1 x_2^0 x_3^\alpha \oplus x_1^\alpha x_2^\alpha x_3^0 \oplus x_1^\alpha x_2^\alpha x_3^1.$$

It is easy to check that in the both cases $\alpha = 1$ and $\alpha = 0$ the function f is symmetric. Hence there exist exactly two functions from P_2^2 in the form (3) with $\alpha = \beta$. These two functions are realized in the case **A.b.2**.

Finally, let us consider the functions in the form

$$(5) \quad f = x_3^\alpha (x_1^0 x_2^1 \oplus x_1^1 x_2^0) \oplus x_1^{\neg\alpha} x_2^{\neg\alpha}.$$

Since $f(\alpha, \beta, \neg(\alpha)) = 0$ and $f(\neg(\alpha), \beta, \alpha) = 1$ for all $\beta \in \{0, 1\}$ it follows that f is not symmetric with respect to x_1 and x_3 . Furthermore, it is clear that f is symmetric with respect to x_1 and x_2 . Hence there are exactly six functions from P_2^3 in the form (5). When $\alpha = 1$ we obtain three function by three permutations of the variables and the same number functions for $\alpha = 0$. These functions are realized in the cases: **A.a.2.**, **B.a.1.** and **B.b.2**. ■

Lemma 3.1. *Let $f = x_4^0 \cdot g(x_1, x_2, x_3) \oplus x_4^1 \cdot h(x_1, x_2, x_3) \in P_2^4$. If $f \in G_2^4$, then $\text{ess}(g_{i \leftarrow j}) < 2$ and $\text{ess}(h_{i \leftarrow j}) < 2$ for all i, j , $1 \leq i < j \leq 3$.*

Proof. Let us suppose that the lemma is false. Without loss of generality let us assume $\text{ess}(g_{2 \leftarrow 1}) \geq 2$. If $f \in G_2^4$, then $x_4 \notin \text{Ess}(f_{2 \leftarrow 1})$ because

$$f_{2 \leftarrow 1} = x_4^0 \cdot g_{2 \leftarrow 1} \oplus x_4^1 \cdot h_{2 \leftarrow 1} \quad \text{and} \quad f_{2 \leftarrow 1}(x_4 = 0) = g_{2 \leftarrow 1}.$$

From Theorem 2.2 it follows that $g_{2 \leftarrow 1} = h_{2 \leftarrow 1}$. Let us set

$$g := \bigoplus_{m=0}^7 a_m^{(0)} \cdot x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} \quad \text{and} \quad h := \bigoplus_{m=0}^7 a_m^{(1)} \cdot x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3},$$

where $m = \overline{\alpha_1 \alpha_2 \alpha_3}$, and

$$t := a_0^{(0)} \cdot x_1^0 x_2^0 x_3^0 \oplus a_1^{(0)} \cdot x_1^0 x_2^0 x_3^1 \oplus a_6^{(0)} \cdot x_1^1 x_2^1 x_3^0 \oplus a_7^{(0)} \cdot x_1^1 x_2^1 x_3^1.$$

Then from $g_{2 \leftarrow 1} = h_{2 \leftarrow 1}$, we obtain

$$g := t(x_1, x_2, x_3) \oplus \left(\bigoplus_{\alpha_1 \neq \alpha_2} a_m^{(0)} \cdot x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} \right) \quad \text{and}$$

$$h := t(x_1, x_2, x_3) \oplus \left(\bigoplus_{\alpha_1 \neq \alpha_2} a_m^{(1)} x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} \right).$$

Note that

$$f_{2 \leftarrow 1} = t_{2 \leftarrow 1} = g_{2 \leftarrow 1} = h_{2 \leftarrow 1}.$$

If $\text{ess}(g_{2 \leftarrow 1}) > 2$, then from $f_{2 \leftarrow 1}(x_4 = 0) = g_{2 \leftarrow 1}$ it follows that $f \notin G_2^4$.

Hence $\text{ess}(g_{2 \leftarrow 1}) = 2$. Thus we have $\{x_1, x_3\} = \text{Ess}(g_{2 \leftarrow 1})$. This implies

$$(6) \quad (a_0^{(0)}, a_6^{(0)}) \neq (a_1^{(0)}, a_7^{(0)}) \text{ and } (a_0^{(0)}, a_1^{(0)}) \neq (a_6^{(0)}, a_7^{(0)}).$$

From $x_4 \in \text{Ess}(f)$ it follows that there are three numbers $\alpha_1, \alpha_2, \alpha_3 \in \{0, 1\}$ such that $a_m^{(0)} \neq a_m^{(1)}$ where $m = \overline{\alpha_1 \alpha_2 \alpha_3}$. Then $\alpha_1 \neq \alpha_2$. Hence we have $\alpha_1 = \alpha_3$ or $\alpha_2 = \alpha_3$.

Let us assume $\alpha_1 = \alpha_3$. Then the identification minor $u = f_{3 \leftarrow 1}$ can be written as follows

$$u = a_0^{(0)} x_1^0 x_2^0 \oplus a_7^{(0)} x_1^1 x_2^1 \oplus x_4^0 (a_2^{(0)} x_1^0 x_2^1 \oplus a_5^{(0)} x_1^1 x_2^0) \oplus x_4^1 (a_2^{(1)} x_1^0 x_2^1 \oplus a_5^{(1)} x_1^1 x_2^0).$$

Without loss of generality let us assume that $a_2^{(0)} \neq a_2^{(1)}$, i.e. $m = \overline{010} = 2$. (Alternative opportunity is $m = 5$.) Then we have $a_2^{(0)} \neq 0$ or $a_2^{(1)} \neq 0$. Again, without loss of generality let us assume $a_2^{(0)} = 1$ and $a_2^{(1)} = 0$. Then $u(x_1 = \alpha_1, x_2 = \alpha_2) = a_2^{(0)} x_4^0 \oplus a_2^{(1)} x_4^1$. Hence $x_4 \in \text{Ess}(u)$.

On the other hand we have

$$u_1 = u(x_4 = 0) = a_0^{(0)} x_1^0 x_2^0 \oplus a_7^{(0)} x_1^1 x_2^1 \oplus x_1^0 x_2^1 \oplus a_5^{(0)} x_1^1 x_2^0 \text{ and}$$

$$u_2 = u(x_4 = 1) = a_0^{(0)} x_1^0 x_2^0 \oplus a_7^{(0)} x_1^1 x_2^1 \oplus a_5^{(1)} x_1^1 x_2^0.$$

Thus we have:

If $a_0^{(0)} = a_7^{(0)} = 0$ or $a_0^{(0)} = a_7^{(0)} = 1$, then $\text{Ess}(u_1) = \{x_1, x_2\}$.

Let $a_0^{(0)} \neq a_7^{(0)}$. Then according to (6) we can assume without loss of generality that $a_0^{(0)} = 1$ and $a_7^{(0)} = 0$. Now, we have:

If $a_5^{(0)} = 1$ or $a_5^{(1)} = 0$, then $\text{Ess}(u_1) = \{x_1, x_2\}$ or $\text{Ess}(u_2) = \{x_1, x_2\}$.

Finally, if $a_0^{(0)} = 1$, $a_7^{(0)} = 0$, $a_5^{(0)} = 0$ and $a_5^{(1)} = 1$ we have $u_1(x_1, x_2) = x_1^0$ and $u_2(x_1, x_2) = x_2^0$.

So, we have shown that $\text{Ess}(u) = \{x_1, x_2, x_4\}$. Hence $f \notin G_2^4$, which is a contradiction.

By symmetry, we obtain the same contradiction when $\alpha_2 = \alpha_3$ and we have to use the identification minor $v = f_{3 \leftarrow 2}$ instead of $u = f_{3 \leftarrow 1}$. \blacksquare

Lemma 3.2. Let $f = x_4^0 g(x_1, x_2, x_3) \oplus x_4^1 h(x_1, x_2, x_3) \in P_2^4$. If $f \in G_2^4$, then $\text{ess}(g) = \text{ess}(h) = 3$.

Proof. Let us suppose that $x_3 \notin \text{Ess}(g)$ and $f \in G_2^4$.

Let g and h are represented as follows

$$g := \bigoplus_{m=0}^7 a_m x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} \text{ and } h := \bigoplus_{m=0}^7 b_m x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3},$$

where $m = \overline{\alpha_1 \alpha_2 \alpha_3} = \alpha_1 \cdot 2^2 + \alpha_2 \cdot 2 + \alpha_3$. Since $x_3 \notin \text{Ess}(g)$, we obtain

$$(7) \quad (a_0, a_2, a_4, a_6) = (a_1, a_3, a_5, a_7).$$

On the other hand $x_3 \notin \text{Ess}(g)$ implies $x_3 \in \text{Ess}(h)$. Hence, we have

$$(8) \quad (b_0, b_2, b_4, b_6) \neq (b_1, b_3, b_5, b_7).$$

Without loss of generality let us assume that $b_0 = 1$ and $b_1 = 0$. Consequently,

$$u = f_{2 \leftarrow 1} = x_4^0(a_0x_1^0 \oplus a_6x_1^1) \oplus x_4^1(x_1^0x_3^0 \oplus b_6.x_1^1x_3^0 \oplus b_7x_1^1x_3^1).$$

From $u(x_1 = 0, x_4 = 1) = x_3^0$ it follows $x_3 \in \text{Ess}(u)$. If $a_0 = 1$, then $u(x_1 = 0, x_3 = 1) = x_4^0$ and if $a_0 = 0$, then $u(x_1 = 0, x_3 = 0) = x_4^1$. Hence $x_4 \in \text{Ess}(u)$. The proof will be done if we show that $x_1 \in \text{Ess}(u)$. Suppose the opposite i.e. $x_1 \notin \text{Ess}(u)$. From Theorem 2.2 it follows that $a_0 = a_6$, $b_6 = 1$ and $b_7 = 0$. Then we have

$$\begin{aligned} v = f_{3 \leftarrow 1} &= x_4^0[a_0.(x_1^0x_2^0 \oplus x_1^1x_2^1) \oplus a_2.x_1^0x_2^1 \oplus a_4.x_1^1x_2^0] \oplus \\ &\oplus x_4^1[x_1^0x_2^0 \oplus b_2.x_1^0x_2^1 \oplus b_5.x_1^1x_2^0]. \end{aligned}$$

If $a_0 = 1$, then $v(x_1 = 1, x_2 = 1) = x_4^0$ and if $a_0 = 0$, then $v(x_1 = 0, x_2 = 0) = x_4^1$. Hence $x_4 \in \text{Ess}(v)$. On the other side it is clear that $v(x_4 = 1) := x_1^0x_2^0 \oplus b_2.x_1^0x_2^1 \oplus b_5.x_1^1x_2^0$ is not a constant. Assume that $x_2 \in \text{Ess}(v)$. Suppose that $x_1 \notin \text{Ess}(v)$. Hence $a_0 = a_2 = a_4$, $b_5 = 1$ and $b_2 = 0$. Thus we obtain

$$w = f_{3 \leftarrow 2} = a_0.x_4^0 \oplus x_4^1(x_1^0x_2^0 \oplus b_3.x_1^0x_2^1 \oplus b_4.x_1^1x_2^0).$$

Clearly $x_4 \in \text{Ess}(w)$. On the other hand it is clear that $w(x_4 = 1) := x_1^0x_2^0 \oplus b_3.x_1^0x_2^1 \oplus b_4.x_1^1x_2^0$ is not a constant. Assume that $x_2 \in \text{Ess}(w)$. Suppose that $x_1 \notin \text{Ess}(w)$. Hence $b_3 = 0$ and $b_4 = 1$. Thus finally, we obtain

$$f = a_0.x_4^0 \oplus x_4^1(x_1^0x_2^0x_3^0 \oplus x_1^1x_2^0x_3^0 \oplus x_1^1x_2^0x_3^1 \oplus x_1^1x_2^1x_3^0).$$

The contradiction is $f \notin G_2^4$ because $f_{4 \leftarrow 2} = a_0.x_2^0 \oplus x_1^1x_2^1x_3^0$.

By analogy we conclude that $f \notin G_2^4$ for the all other cases generated by (7) and (8), which is a contradiction. \blacksquare

Theorem 3.3. *Let $f \in P_2^4$. Then $f \in G_2^4$ if and only if $f = x_4^0.g(x_1, x_2, x_3) \oplus x_4^1.h(x_1, x_2, x_3)$, with*

$$(9) \quad g = x_3^\alpha(x_1^0x_2^0 \oplus x_1^1x_2^1) \oplus x_3^{-\alpha}(x_1^0x_2^1 \oplus x_1^1x_2^0),$$

and

$$(10) \quad h = x_3^{-\alpha}(x_1^0x_2^0 \oplus x_1^1x_2^1) \oplus x_3^\alpha(x_1^0x_2^1 \oplus x_1^1x_2^0),$$

for some α , $\alpha \in \{0, 1\}$.

Proof. " \Leftarrow " The proof in this direction is done in Proposition 3.2.

" \Rightarrow " Suppose that some of the equations (9) or (10) are not satisfied. From Lemma 3.1 and Lemma 3.2 there are two possible cases:

A.

$$g = x_3^\alpha(x_1^0x_2^1 \oplus x_1^1x_2^0) \oplus x_1^\beta x_2^\beta,$$

and

$$h = x_3^\gamma(x_1^0x_2^0 \oplus x_1^1x_2^1) \oplus x_3^{-\gamma}(x_1^0x_2^1 \oplus x_1^1x_2^0).$$

Then we have the following identification minor of f :

$$u = f_{4 \leftarrow 1} = x_1^0x_2^1x_3^\alpha \oplus \neg(\beta).x_1^0x_2^0 \oplus x_1^1x_2^1x_3^\gamma \oplus x_1^1x_2^0x_3^{-\alpha}.$$

Since $u(x_1 = 0) = x_2^1x_3^\alpha \oplus \neg(\beta).x_2^0$ it follows that $\{x_2, x_3\} \subseteq \text{Ess}(u)$. We will show that $x_1 \in \text{Ess}(u)$, also.

Let $\beta = 0$. If $\gamma = \alpha$, then we have $u(x_2 = 0, x_3 = \gamma) = x_1^0$, and if $\gamma \neq \alpha$, then we have $u(x_2 = 1, x_3 = \gamma) = x_1^1$.

Let $\beta = 1$. If $\gamma = \alpha$, then $u(x_2 = 0, x_3 = \neg(\gamma)) = x_1^1$, and if $\gamma \neq \alpha$, then we have $u(x_2 = 1, x_3 = \gamma) = x_1^1$.

Hence $x_1 \in \text{Ess}(u)$ and $f \notin G_2^4$ in the case **A**.

B.

$$g = x_3^\alpha(x_1^0x_2^1 \oplus x_1^1x_2^0) \oplus x_1^\beta x_2^\beta,$$

and

$$h = x_3^\gamma(x_1^0x_2^1 \oplus x_1^1x_2^0) \oplus x_1^\delta x_2^\delta.$$

Since $x_4 \in \text{Ess}(f)$ it follows that $g \neq h$.

Let us consider the identification minor u of f , also:

$$u = f_{4 \leftarrow 1} = x_1^\alpha x_2^\alpha x_3^\alpha \oplus \neg(\beta).x_1^0 x_2^0 \oplus x_1^1 x_2^0 x_3^\gamma \oplus \delta.x_1^1 x_2^1.$$

Since $u(x_1 = 0) = x_2^\alpha x_3^\alpha \oplus \neg(\beta).x_2^0$ it follows that $\{x_2, x_3\} \subseteq \text{Ess}(u)$. We will prove that $x_1 \in \text{Ess}(u)$, also.

Let $\beta = \delta = 0$. Then $u(x_2 = 1, x_3 = \alpha) = x_1^0$;

Let $\beta = \delta = 1$. Then $u(x_2 = 0, x_3 = \gamma) = x_1^1$;

Let $\beta = 1$ and $\delta = 0$. Then $u(x_2 = 0, x_3 = \gamma) = x_1^1$;

Let $\beta = 0$ and $\delta = 1$. Then $u(x_2 = 1, x_3 = \neg(\alpha)) = x_1^1$.

Hence $x_1 \in \text{Ess}(u)$ and $f \notin G_2^4$ in the case **B.**, also. This is a contradiction. \blacksquare

Remark 1. Note that g and h have to be two special functions from G_2^3 , represented by the equation (4) of Theorem 3.2. Such functions can be obtained in the cases of the same theorem **B.a.2** and **B.b.2**, only.

Corollary 3.5. Let $f \in P_2^4$. Then $f \in G_2^4$ if and only if $f = x_4^0.g(x_1, x_2, x_3) \oplus x_4^1.h(x_1, x_2, x_3)$, with

$$g = x_3^\alpha(x_1^0x_2^0 \oplus x_1^1x_2^1) \oplus x_3^{\neg(\alpha)}(x_1^0x_2^1 \oplus x_1^1x_2^0),$$

and $h = \neg(g(x_1, x_2, x_3))$.

Corollary 3.6. Let $f \in P_2^4$. Then $f \in G_2^4$ if and only if

$$f = a_0. \left(\bigoplus_{\alpha_1 \alpha_2 \alpha_3 \alpha_4 \in \text{Od}_2^4} x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} x_4^{\alpha_4} \right) \oplus \neg(a_0). \left(\bigoplus_{\alpha_1 \alpha_2 \alpha_3 \alpha_4 \in \text{Ev}_2^4} x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3} x_4^{\alpha_4} \right).$$

Corollary 3.7. If $f \in G_2^4$ then $x_j \notin \text{Ess}(f_{i \leftarrow j})$ for all $i, j \in \{1, 2, 3, 4\}$ $i \neq j$.

Proof. The three corollaries, above can be proved by immediate checking of the both functions from G_2^4 , obtained in Theorem 3.3. \blacksquare

Theorem 3.4. A Boolean function $f \in P_2^n$, depending on n essential variables with $n \geq 4$, has essential arity gap 2 if and only if

$$f = \bigoplus_{\alpha_1 \dots \alpha_n \in \text{Od}_2^n} x_1^{\alpha_1} \dots x_n^{\alpha_n} \quad \text{or} \quad f = \bigoplus_{\alpha_1 \dots \alpha_n \in \text{Ev}_2^n} x_1^{\alpha_1} \dots x_n^{\alpha_n}.$$

Proof. " \Leftarrow " In this direction the proof is done by Proposition 3.2.

" \Rightarrow " We will proceed by induction on n . If $n = 4$ the theorem is true because of Theorem 3.3. Suppose that if $4 \leq n \leq l$ and $f \in G_2^n$, then

$$f = \bigoplus_{\alpha_1 \dots \alpha_n \in \text{Od}_2^n} x_1^{\alpha_1} \dots x_n^{\alpha_n} \quad \text{or} \quad f = \bigoplus_{\alpha_1 \dots \alpha_n \in \text{Ev}_2^n} x_1^{\alpha_1} \dots x_n^{\alpha_n}.$$

Let $f \in G_2^{l+1}$. Hence f can be presented as follows

$$f = x_{l+1}^0.g(x_1, \dots, x_l) \oplus x_{l+1}^1.h(x_1, \dots, x_l).$$

In the same way as in Lemma 3.1 and Lemma 3.2 it can be proved that $g, h \in G_2^l$. By the inductive supposition g and h are functions of the forms

$$\bigoplus_{\gamma_1 \dots \gamma_l \in Od_2^l} x_1^{\gamma_1} \dots x_l^{\gamma_l} \quad \text{or} \quad \bigoplus_{\gamma_1 \dots \gamma_l \in Ev_2^l} x_1^{\gamma_1} \dots x_l^{\gamma_l},$$

with $g \neq h$. Note that g and h are not constants because $ess(f) = n \geq 4$. Hence $Ess(g_{i \leftarrow j}) = Ess(h_{i \leftarrow j})$ for $i, j \in \{1, \dots, l\}$ and $i \neq j$. Assume that

$$g = \bigoplus_{\gamma_1 \dots \gamma_l \in Od_2^l} x_1^{\gamma_1} \dots x_l^{\gamma_l} \quad \text{and} \quad h = \bigoplus_{\delta_1 \dots \delta_l \in Ev_2^l} x_1^{\delta_1} \dots x_l^{\delta_l}.$$

Consequently

$$\begin{aligned} f &= x_{l+1}^0 \cdot \left(\bigoplus_{\gamma_1 \dots \gamma_l \in Od_2^l} x_1^{\gamma_1} \dots x_l^{\gamma_l} \right) \oplus x_{l+1}^1 \cdot \left(\bigoplus_{\delta_1 \dots \delta_l \in Ev_2^l} x_1^{\delta_1} \dots x_l^{\delta_l} \right) = \\ &= \bigoplus_{\alpha_1 \dots \alpha_{l+1} \in Od_2^{l+1}} x_1^{\alpha_1} \dots x_{l+1}^{\alpha_{l+1}}. \end{aligned}$$

The case $g = h$ is impossible because $ess(f) = l + 1$, but the replacement of g and h will produce the function

$$f = \bigoplus_{\alpha_1 \dots \alpha_l \in Ev_2^l} x_1^{\alpha_1} \dots x_l^{\alpha_l},$$

which does not depend on x_{l+1} . ■

Corollary 3.8. *A Boolean function $f \in P_2^n$, which essentially depends on n variables with $n > 4$, has essential arity gap 2 if and only if*

$$f = x_n^0 \cdot g(x_1, \dots, x_i, \dots, x_{n-1}) \oplus x_n^1 \cdot g(x_1, \dots, x_{i-1}, \neg(x_i), x_{i+1}, \dots, x_{n-1}),$$

where $g \in G_2^{n-1}$ and $i \in \{1, \dots, n-1\}$.

Proof. If

$$g = \bigoplus_{\gamma_1 \dots \gamma_{n-1} \in Od_2^{n-1}} x_1^{\gamma_1} \dots x_{n-1}^{\gamma_{n-1}} \quad \text{and} \quad h = \bigoplus_{\gamma_1 \dots \gamma_{n-1} \in Od_2^{n-1}} x_1^{\gamma_1} \dots x_{n-1}^{\gamma_{n-1}},$$

then $\neg(g) = h$ and $\neg(h) = g$ for all $l \geq 4$. On the other hand, for each $i \in \{1, \dots, n-1\}$, we have

$$\neg(g) = \bigoplus_{\gamma_1 \dots \gamma_{n-1} \in Od_2^{n-1}} x_1^{\gamma_1} \dots x_{i-1}^{\gamma_{i-1}} \neg(x_i^{\gamma_i}) x_{i+1}^{\gamma_{i+1}} \dots x_{n-1}^{\gamma_{n-1}}.$$

■

Corollary 3.9. $|G_2^n| = 2$ for each $n, n \geq 4$.

One of the most important problems concerning the essential arity gap is to calculate the number of all functions from P_2^n , which depend essentially on at most n variables and which have the maximum gap i.e. with gap equal to 2. The next theorem gives answer of that problem. It summarize the results obtained above in the paper.

Let us denote by H_n the set of all functions in P_2^n , which have gap equal to 2 i.e.

$$H_n := \bigcup_{m=2}^n G_2^m \quad \text{and} \quad h_n := |H_n|.$$

Theorem 3.5. *The following combinatorial equations are held:*

- (i) $h_2 = 6$;
- (ii) $h_3 = 28$;
- (iii) $h_n = 3 \cdot \binom{n}{2} + 5 \cdot \binom{n}{3} + 2^{n+1} - 2n - 2$, when $n \geq 4$;

Proof.

(i) follows from Corollary 3.1 of Theorem 3.1;

(ii) Let $X_3 = \{x_1, x_2, x_3\}$. There are $6 \cdot \binom{3}{2}$ Boolean functions with essential arity gap equal to 2, which depend essentially on 2 variables from X_3 , according to Corollary 3.1 of Theorem 3.1.

From Corollary 3.4 of Theorem 3.2 it follows that there are 10 Boolean functions with essential arity gap equal to 2, which depend essentially on all 3 variables from X_3 . Hence $h_3 = 6 \cdot 3 + 10 = 28$.

(iii) Let $X_n = \{x_1, \dots, x_n\}$, $n \geq 4$. There are $6 \cdot \binom{n}{2}$ Boolean functions with essential arity gap equal to 2, which depend essentially on 2 variables from X_n , according to Corollary 3.1 of Theorem 3.1.

There are $10 \cdot \binom{n}{3}$ Boolean functions with essential arity gap equal to 2, which depend essentially on 3 variables from X_n , according to Corollary 3.4 of Theorem 3.2.

Finally, for each m , $3 < m \leq n$ there are $2 \cdot \binom{n}{m}$ Boolean functions with essential arity gap equal to 2, which depend essentially on m variables from X_n , according to Corollary 3.9 of Theorem 3.4.

Hence we have

$$\begin{aligned} h_n &= 6 \cdot \binom{n}{2} + 10 \cdot \binom{n}{3} + 2 \cdot \left[\binom{n}{4} + \binom{n}{5} + \dots + \binom{n}{n} \right] = \\ &= 3 \cdot \binom{n}{2} + 5 \cdot \binom{n}{3} + 2^{n+1} - 2n - 2. \end{aligned}$$

■

REFERENCES

- [1] Yu. Breitbart, *On the essential variables of functions in the algebra of logic*, Dokl. Acad. Sci. USSR, 172, v. 1, 1967, 9-10 (in Russian).
- [2] K. Chimev, *Separable Sets of Arguments of Functions*, MTA SzTAKI Tanulmányok, 180/1986, 173 pp.
- [3] M. Couceiro, E. Lehtonen, *On the effect of variable identification on the essential arity of functions on finite sets*, Int. Journal of Foundations of Computer Science, vol. 18, Issue 5, (October 2007), 975-986.
- [4] A. Salomaa, *On Essential Variables of Functions, Especially in the Algebra of Logic*, Annales Academia Scientiarum Fennicae, Ser. A, 333, 1963, 1-11.
- [5] O. Lupanov, *On a class schemas of functional elements*, Problemi Cybernetiki, 9, 1963, 333-335 (in Russian).
- [6] Sl. Shtrakov, *Tree Automata and Essential Input Variables*, Contributions to General Algebra 13, Verlag Johannes Heyn, Klagenfurt, 2001, pp.309-320.
- [7] Sl. Shtrakov, K. Denecke, *Essential Variables and Separable Sets in Universal Algebra*, Taylor & Francis, Multiple-Valued Logic, An International Journal, vol. 8, No.2, 2002, 165-182.

E-mail address: shtrakov@aix.swu.bg

DEPARTMENT OF COMPUTER SCIENCE, SOUTH-WEST UNIVERSITY, 2700 BLAGOEVGRAD, BULGARIA

URL: <http://home.swu.bg/shtrakov>